

## Workshop focuses on detecting attacks

*by Francis L. Crumb, Information Directorate*

ROME, N.Y. — Timely methods to detect and investigate cyber attacks was the focus of the 4<sup>th</sup> Annual Digital Forensic Research Workshop (DFRWS), sponsored by the Air Force Research Laboratory Information Directorate Aug. 10-13 at Linthicum, Md.

Workshop participation included more than 100 leading researchers, practitioners and developers from Australia, Italy, the Netherlands, Uganda, the United Kingdom and the United States. Attendees drew from a nearly equal base of Department of Defense researchers, law enforcement, industry and academia.

Mark Pollitt, former director of the FBI Computer Analysis and Response Team, and Lance Spitzner of the HoneyNet Project, a non-profit research organization of security professionals dedicated to information security, were the keynote speakers. In addition to the keynote addresses, the workshop featured 13 papers and two panel discussions.

“DFRWS activities center around the need to enhance and promote the application of the scientific method in research and practice in digital forensic science,” said Chester J. Maciag, an electronics engineer in the directorate’s Defensive Information Warfare Branch. “As such, efforts strive to discover, define and foster fundamental scientific principles that will support investigations of digital ‘wrongdoing’ from all perspectives.

The DFRWS was initiated in August 2001 to bring academic researchers and digital forensic investigators and practitioners together to define the need and create the processes for the incorporation of a rigorous scientific method as a fundamental tenant of the evolving discipline of digital forensic science. Participants also developed a research agenda that considered practitioner requirements, multiple investigative environments and emphasizes real world usability.

“We have a goal of discovery, explanation and presentation of conclusive, persuasive evidence that will meet the heightened scrutiny of the courts and other decision-makers in military and civilian environments,” said Mr. Maciag.

During the next year, DFRWS will be exploring a variety of topics through mini-workshops that will address other challenging topics such a remote digital investigation, data mining and situational awareness. @